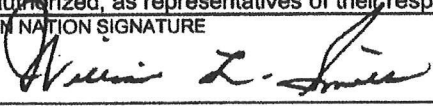
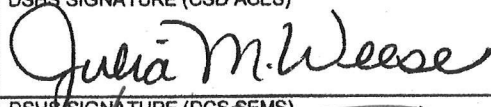
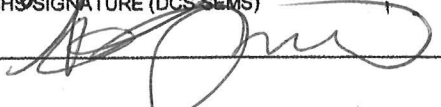
		INDIAN NATION PROGRAM AGREEMENT DATA SHARE AGREEMENT ACES & SEMS WEB		DSHS Agreement Number 1462-11433
This Program Agreement is by and between the State of Washington Department of Social and Health Services (DSHS) and the Indian Nation identified below, and is issued in conjunction with the DSHS and Indian Nation Agreement Regarding General Terms and Conditions, which is incorporated by reference.				Administration or Division Agreement Number Indian Nation Agreement Number
DSHS ADMINISTRATION Economic Services Administration	DSHS DIVISION Office of the Assistant Secretary	DSHS INDEX NUMBER 3214	CCS CONTRACT CODE 3042NS-62	
DSHS CONTACT NAME AND TITLE Mike Mowrey Program Administrator		DSHS CONTACT ADDRESS PO Box 45857 Olympia, WA 98504-5857		
DSHS CONTACT TELEPHONE (360) 725-4656	DSHS CONTACT FAX (360) 413-3123	DSHS CONTACT E-MAIL mowrems@dsHS.wa.gov		
INDIAN NATION NAME South Puget Intertribal Planning Agency		INDIAN NATION ADDRESS 3104 SE Old Olympic Hwy Shelton, WA 98584-7731		
INDIAN NATION CONTACT NAME Whitney Jones				
INDIAN NATION CONTACT TELEPHONE (360) 426-3990	INDIAN NATION CONTACT FAX	INDIAN NATION CONTACT E-MAIL wjones@spipa.org		
IS THE INDIAN NATION A SUBRECIPIENT FOR PURPOSES OF THIS PROGRAM AGREEMENT? No		CFDA NUMBERS		
PROGRAM AGREEMENT START DATE 06/01/2014	PROGRAM AGREEMENT END DATE 08/31/2016	MAXIMUM PROGRAM AGREEMENT AMOUNT \$0.00		
EXHIBITS. When the box below is marked with a check (✓) or an X, the following Exhibits are attached and are incorporated into this Indian Nation Program Agreement by reference: <input checked="" type="checkbox"/> Data Security: Exhibit A – Data Security Requirements <input checked="" type="checkbox"/> Exhibits (specify): Exhibit B – Assurances & Certifications form, Exhibit C – Washington State Department of Social & Health Services – Notice of Nondisclosure, Exhibit D – DSHS Form 9-989 (Confidentiality Statement – Tribal Employee)				
By their signatures below, the parties agree to the terms and conditions of this Indian Nation Program Agreement and all documents incorporated by reference. No other understandings or representations, oral or otherwise, regarding the subject matter of this Program Agreement shall be deemed to exist or bind the parties. The parties signing below certify that they are authorized, as representatives of their respective governments, to sign this Program Agreement.				
INDIAN NATION SIGNATURE 		PRINTED NAME AND TITLE WILLIAM L. SMITH EXECUTIVE DIRECTOR	DATE SIGNED 3/30/2014	
DSHS SIGNATURE (CSD ACES) 		PRINTED NAME AND TITLE Julia M. Weese, Contracts Risk Manager Department of Social and Health Services Economic Services Administration (ESA)	DATE SIGNED 6/11/14	
DSHS SIGNATURE (DCS SEMS) 		PRINTED NAME AND TITLE Ann Polanco, Contracts Administrator ESA / Division of Child Support	DATE SIGNED 6/11/14	

Administration.

b. Purpose

(1) The purpose of this agreement is to provide access to data for the limited purpose of assisting SPIPA in administering their Tribal Title IV-A TANF Program, DSHS shall provide SPIPA with access to:

- (a) Automated Client Eligibility System (ACES)
- (b) Support Enforcement Management System (SEMS)
- (c) Employment Security Department (ESD) earnings and benefit information.

Tribal TANF staff must only access ESD through ACES.

c. Description of Data

(1) ACES Data

Designated employees or contracted staff of SPIPA shall have limited read-only web based secured access to ACES.

(2) SEMS Data

Designated employees or contracted staff of SPIPA shall have limited read-only web based secured access to SEMS cases where SPIPA is coded on the SEMS case. DSHS will provide SPIPA's staff with electronic inquiry only access to Child Support information for verification of child support cases, family relationships, and financial history as authorized under RCW 26.23.120. The IV-D data in SEMS that DCS may provide to a Tribal IV-A program is limited to the purposes provided for in 45 CFR 307.13.

(3) Confidential Benefit and Wage Employment Data

Designated employees or contracted staff of SPIPA shall have limited read-only web based secured access to confidential benefit and wage employment data collected through the Unemployment Compensation (UC) program, which is accessed through ACES.

d. Data Access or Transfer

(1) Unique user identification numbers and passwords obtained from DSHS are required in order for the authorized SPIPA staff to log on to ACES and SEMS.

(2) SPIPA will need to submit the IP numbers of the workstations that will need to access ACES and SEMS.

(3) ACES/SEMS - Method of Access / Transfer

(a) Connection to ACES and SEMS will occur in one of the following two ways, either:

- i. Through a workstation attached to the intergovernmental network (IGN), or
- ii. DSHS will grant data access to ACES and SEMS for designated staff through a Virtual Private Network (VPN) connection provided by the Information System Services Division

(ISSD), which uses fobs or software security tokens (SST) as a secondary factor of authentication, in addition to user identification and password.

(A) SPIPA will elect whether the secondary factor of authentication will be either fobs or SSTs.

(B) If SPIPA opts to use fobs:

1. DSHS will provide a maximum of six (6) dual ACES-SEMS fobs to the Tribal TANF program free of charge. Each of the six (6) fobs will provide access to both ACES & SEMS.
2. Each of the fobs provided must be assigned to only one (1) individual, and access and use of the fobs shall not be shared between program employees or contracted staff.
3. Fobs lost or damaged by SPIPA may be replaced by DSHS. DSHS may charge SPIPA \$75.00 to replace a lost or damaged fob.

(C) If SPIPA opts to use SST's:

1. DSHS will provide a maximum of six (6) dual ACES-SEMS SST's to the Tribal TANF program free of charge. Each of the six (6) SST's will provide access to both ACES & SEMS.
2. Each of the SST's provided must be assigned to only one (1) individual, and access and use of the SST's shall not be shared between program employees or contracted staff.

(b) SPIPA shall ensure that:

Tribal TANF program employees or contracted staff access wage and UC information from the ESD only through ACES.

e. Limitations on Use of Data

(1) SPIPA shall ensure that Tribal TANF employees or contracted staff persons have access to ACES and SEMS records only when necessary to fulfill the TANF requirements of their program.

(2) ACES – SEMS Security Monitoring

(a) SPIPA shall assign a person as a security monitor as a point of contact for ACES and SEMS.

(b) The security monitor will:

- i. Route ACES access requests through the ESA Information Technology Division Central Support Help Desk.
- ii. Route SEMS access requests through the DCS Program Manager.
- iii. Assist in DSHS' efforts to monitor the security provisions of the DSA, by annually reviewing, completing and submitting the Assurances and Certifications form (see

Exhibit B) to DSHS on the following dates:

(A) June 1, 2014

(B) June 1, 2015

- iv. Notify the ESA Information Technology Division Central Support Help Desk immediately when employees or contracted staff that have access to ACES terminate employment, transfer, or change duties.
- v. Notify the DCS Program Manager immediately when employees or contracted staff that have access to SEMS terminate employment, transfer, or change duties.
- vi. Perform the following actions upon an employee or contracted staff member (with SEMS or ACES access) terminating employment, transferring, or changing duties:

(A) Promptly revoke access that is no longer needed or appropriate. Disable (revoke) all user IDs within five business days of the termination.

(B) Notify the employee or contracted staff member of his or her duty to keep information confidential.

(C) Disable (revoke) all access and user IDs immediately when an employee or contracted staff member is terminated for cause.

(c) Supervisors and/or managers must promptly report to the security monitor duty changes or other personnel changes for which removal or reduction of computer system privileges is appropriate.

f. Frequency of Exchange

The exchange of data is accomplished through on-line transactions that may occur whenever the application is available

g. Security of Data

(1) SPIPA shall secure the data provided in accordance with the requirements of **Exhibit A – Data Security Requirements**.

(2) SPIPA shall exercise due care to protect data from unauthorized physical and electronic access. Due care includes establishing and maintaining security policies, standards, and procedures which detail:

(a) Access security, identification, and authentication;

(b) Network and workstation security;

(c) Premise security; and

(d) Sanctions for unauthorized use or disclosure of data.

(3) To limit potential security breaches, if a Fob or SST is inactive for more than ninety (90) days, DSHS may deactivate it.

- (4) DSHS provided data stored by SPIPA may not be accessed remotely — no use of external networks (e.g. the Internet) is allowed under this agreement.
- (5) SPIPA shall track the location of any copies or backups of data provided by DSHS. The method of tracking shall be sufficient to provide the ability to audit the protections afforded the copied data sets.
- (6) In the case of hardware failure, SPIPA must protect data by removing the hard drive before shipping equipment for repair.

h. Confidentiality and Nondisclosure:

- (1) SPIPA shall protect confidential information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other State, Federal, or Tribal laws including the following incorporated by reference:

(a) SEMS IV-D Data:

- i. RCW 42.56.230 Personal Information
- ii. RCW 26.23.120 Information & Records – Confidentiality – Disclosure – Adjudicative Proceeding – Rules – Penalties
- iii. 45 CFR 307.13 Security & Confidentiality for Computerized Support Enforcement Systems in Operation After October 1, 1997
- iv. 20 CFR 603 Federal-State Unemployment Compensation (UC) Program, Confidentiality & Disclosure of State UC Information
- v. 42 USC 654(26) Safeguarding Confidential Information

(b) ACES Data:

- i. RCW 74.04.060 Records, Confidential – Exception – Penalty
- ii. RCW 42.56.230 Personal Information
- iii. 42 USC 603 Federal-State Unemployment Compensation (UC) Program, Confidentiality & Disclosure of State UC Information

- (2) For Child Support information contained in SEMS or the Title IV-D program, all information is private and confidential and shall be exempt from disclosure under RCW 42.56 or other Federal, State or Tribal laws.
- (3) SPIPA shall have adequate policies and procedures in place to ensure compliance with confidentiality requirements.
- (4) SPIPA, its employees and contracted staff may use confidential information or data gained by reason of this Agreement only for the purposes of this Agreement.
- (5) SPIPA shall not disclose nor transfer any information as described in this Program Agreement to any party in whole or in part, or to any individual or agency unless the information is exempt from disclosure under applicable State, Federal or Tribal laws.

(6) All confidential information DSHS receives from SPIPA under this Agreement will be kept confidential by DSHS employees as required by State, Federal or Tribal laws.

(7) Notice of Nondisclosure

- (a) ACES: SPIPA must ensure each employee or contracted staff person with access to ACES and/or ESD records or information annually signs the Washington State Department of Social and Health Services, Notice of Nondisclosure (Nondisclosure form) (Exhibit C) prior to DSHS granting access.

SPIPA shall retain a signed copy of the Nondisclosure form on file for monitoring purposes and made available for DSHS review upon request.

- (b) SEMS: SPIPA must ensure that each employee or contracted staff person with SEMS access (including, but not limited to ESD information) annually reviews and signs the Federal and State data access requirements listed in the SEMS, Confidentiality Statement – Tribal Employee (DSHS 9-989) (Exhibit D), prior to DSHS granting access. Staff with direct access must also annually electronically acknowledge this agreement.

SPIPA shall retain a signed copy of the DSHS 9-989 form (**Exhibit D**) on file for monitoring purposes and made available to DSHS review upon request.

(8) Notification of unauthorized disclosure:

SPIPA shall notify the Economic Services Administration (ESA) within one (1) business day of discovery of any unauthorized disclosure of ACES, SEMS or ESD information. Notification to ESA shall be done by sending an email to databreach@dshs.wa.gov.

4. Disputes

Disputes shall be resolved in accordance with the current DSHS and Indian Nation Agreement on General Terms and Conditions between DSHS and the four (4) Tribes participating in the SPIPA Tribal TANF program: Nisqually, Skokomish, Puyallup and Squaxin Island Tribes.

5. Termination

Termination of this Agreement shall be in accordance with the current DSHS and Indian Nation Agreement on General Terms and Conditions between DSHS and the four (4) Tribes participating in the SPIPA Tribal TANF program: Nisqually, Skokomish, Puyallup and Squaxin Island Tribes.

APPROVED AS TO FORM BY THE OFFICE OF THE ATTORNEY GENERAL

Exhibit A – Data Security Requirements

1. **Definitions.** The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:
 - a. "Authorized User(s)" means an individual or individuals with an authorized business requirement to access DSHS Confidential Information.
 - b. "Hardened Password" means a string of at least eight characters containing at least one alphabetic character, at least one number and at least one special character such as an asterisk, ampersand or exclamation point.
 - c. "Unique User ID" means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.
2. **Data Transport.** When transporting DSHS Confidential Information electronically, including via email, the Data will be protected by:
 - a. Transporting the Data within the (State Governmental Network) SGN or Contractor's internal network, or;
 - b. Encrypting any Data that will be in transit outside the SGN or Contractor's internal network. This includes transit over the public Internet.
3. **Protection of Data.** The Contractor agrees to store Data on one or more of the following media and protect the Data as described:
 - a. **Hard disk drives.** Data stored on local workstation hard disks. Access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.
 - b. **Network server disks.** Data stored on hard disks mounted on network servers and made available through shared folders. Access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data as outlined in Section 5. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

- c. **Optical discs (CDs or DVDs) in local workstation optical disc drives.** Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secured Area. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet or other container to which only Authorized Users have the key, combination or mechanism required to access the contents of the container. Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers.** Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secured Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- e. **Paper documents.** Any paper records must be protected by storing the records in a Secured Area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.
- f. **Remote Access.** Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.
- g. **Data storage on portable devices or media.**
 - (1) Except where otherwise specified herein, DSHS Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:
 - (a) Encrypt the Data with a key length of at least 128 bits
 - (b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.
 - (c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
 - Physically Secure the portable device(s) and/or media by
 - (d) Keeping them in locked storage when not in use
 - (e) Using check-in/check-out procedures when they are shared, and

(f) Taking frequent inventories

(2) When being transported outside of a Secured Area, portable devices and media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data.

(3) Portable devices include, but are not limited to; smart phones, tablets, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers if those computers may be transported outside of a Secured Area.

(4) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape), or flash media (e.g. CompactFlash, SD, MMC).

h. Data stored for backup purposes.

(1) DSHS data may be stored on portable media as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DSHS Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements in Section 5. Data Disposition

(2) DSHS Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DSHS Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements in Section 5. Data Disposition.

4. Data Segregation.

- a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.
- b. DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS data. And/or,
- c. DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,
- d. DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,
- e. DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.
- f. When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.

- g. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.

5. **Data Disposition.** When the contracted work has been completed or when no longer needed, except as noted in Section 3. Protection of Data b. Network Server Disks above, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

6. **Notification of Compromise or Potential Compromise.** The compromise or potential compromise of DSHS shared Data must be reported to the DSHS Contact designated in the Contract within one (1) business day of discovery. If no DSHS Contact is designated in the Contract, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.
7. **Data shared with Subcontractors.** If DSHS Data provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract. If the Contractor cannot protect the Data as articulated within this Contract, then the contract with the subcontractor must be submitted to the DSHS Contact specified for this contract for review and approval.

ASSURANCES & CERTIFICATIONS

South Puget Intertribal Planning Agency & State of Washington, Department of Social & Health
ServicesIndian Nation Program Agreement
Data Share Agreement ACES & SEMS Web #1462-1143

1. All TANF program employees or contracted staff members comply with the data security provisions of the Data Share Agreement (DSA).
2. SPIPA has policies in place to ensure confidentiality of ACES and SEMS (including, but not limited to Employment Security Department) data.
3. SEMS Access: All Child Support & TANF program employees or contracted staff members with access to SEMS (including, but not limited to ESD) records and information, whether direct or indirect, have annually signed the DSHS Form 9-989 (Confidentiality Statement – Tribal Employee) (Exhibit D), with a copy kept on file by SPIPA. Staff with direct access must also annually electronically acknowledge this agreement.
4. ACES Access: All Child Support & TANF program employees or contracted staff members with access to DSHS and/or ESD records & information, whether direct or indirect, have annually reviewed and signed the Washington State Department of Social and Health Services, Notice of Nondisclosure form (Exhibit C) with a copy kept on file by SPIPA.
5. Fobs: Each of the Fobs provided by DSHS to SPIPA are assigned to only one (1) individual and access and use of the fobs are not shared between program employees or contracted staff.

TANF Program

- Please identify the four (4) fob users and the Serial Number of the fob assigned to these individuals:

1. <u>Mary DuPuis</u>	Assigned FOB Serial #: <u># 132168615</u>
2. <u>Marla Conwell</u>	Assigned FOB Serial #: <u># 116878877</u>
3. <u>Bryan Blackburn</u>	Assigned FOB Serial #: <u>#116878877</u>
4. <u>Currently unassigned</u>	Assigned FOB Serial #: <u>#</u>

Please check the below box

☒ By checking this box, I agree as SPIPA's Security Monitor for the TANF Program, that SPIPA is in compliance with the certification contained herein.

Marla Conwell
Security Monitor (print name)

Marla Conwell
Security Monitor (signature)

5-28-14
Date